

TITAN

Application Note 44

IPSEC - Client-Server

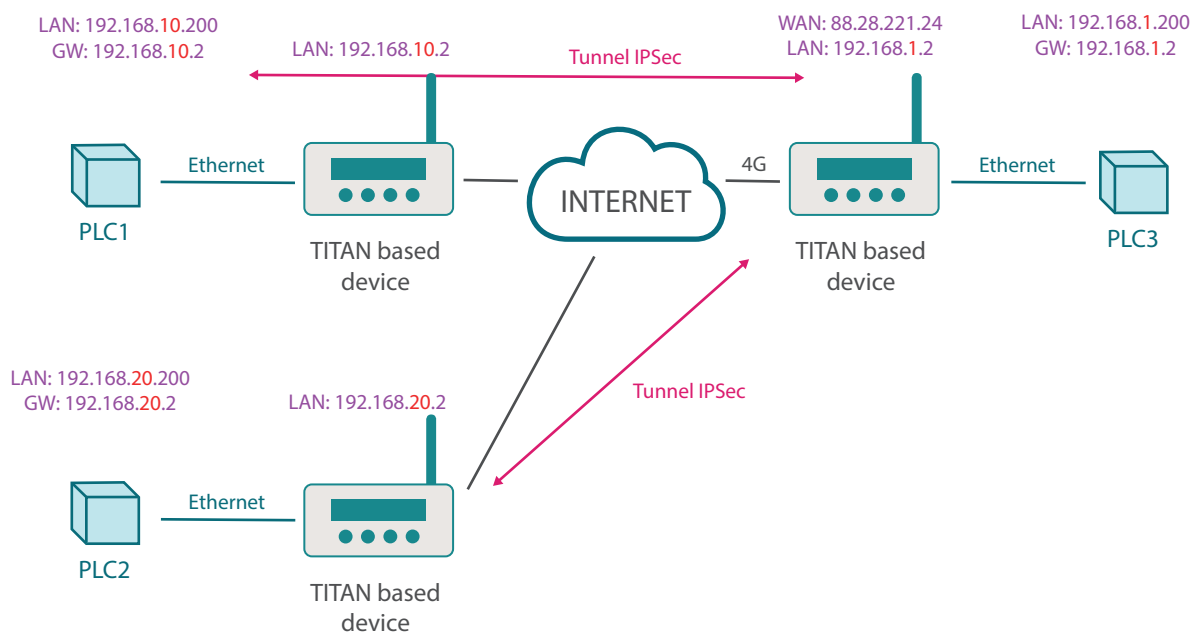
IKEv2 - Authentication Using a Certificate

IPSEC - Client-Server - IKEv2 - Authentication Using a Certificate

1. Scenario Details

We need to implement a secure network between 3 PLCs to enable them to communicate with each other. To do this we will create an IPsec tunnel in which a TITAN-based device connected to the PLC3 will act as the IPsec Master. The TITAN-based device will have a SIM card with a fixed IP address of 88.28.221.24. The TITAN-based devices connected to PLC1 and PLC2 will act as IPsec Clients. The following diagram shows the connection diagram with the relevant IP addresses of all devices.

Example of the proposed scenario:



Digital certificate authentication will be used in this example.

2. Configurations and Prerequisites

The basic requirement for this is that the SIM card inserted in the TITAN-based device acting as the IPsec Server must have public and static IP addresses. This is needed to enable remote access from other TITAN-based devices connected to the Internet. We must also make sure that all the devices are set to the correct time, since the generation and verification of certificates will require this.

3. IPSEC configuration of the TITAN-based device (SERVER)

First we must go to the “VPN > IPSEC” menu. For the planned configuration we will need the “ca-cert.pem”, and “server-cert.pem” certificates. As well as your private keys “ca-key.pem” and “server-key.pem”. We will also need a pair of client certificates with their private keys “client1-cert.pem”, “client1-key.pem”, “client2-cert.pem” and “client2-key.pem”.

At this point there are two options. 1) If these certificates are available, they can be uploaded manually from the section indicated in red:

OpenVPN EasyLink

IPSec

Plugins

- Link
- Nonat
- Wifiscan

Device Manager

- Cervello

Other

- DynDns
- Private DynDns
- Digital Input 1
- Digital Input 2
- ModBus Slave
- Titan Scripts
- Jamming detection
- AT Command
- Sms control
- Email configuration
- Gsm Location
- Periodic Autoreset
- Custom Skin
- Custom Led
- Time Servers
- Advanced Routing
- Remote Console
- Snmp
- Tacacs+
- Mqtt
- Https
- Audio
- User Permissions
- Passwords Web UI
- Backup / Factory
- Firmware Upgrade
- Reboot
- Logout

VPN > IPsec > Client Certificates (files needed for "IPsec client" mode)

CA certificate:	file 'ca1-cert.pem'	Seleccionar archivo	Ningún archivo seleccionado	Upload	not uploaded
Client Certificate:	file 'xclient1-cert.pem'	Seleccionar archivo	Ningún archivo seleccionado	Upload	not uploaded
Client KEY:	file 'xclient1-key.pem'	Seleccionar archivo	Ningún archivo seleccionado	Upload	not uploaded

DELETE ALL CLIENT CERTIFICATES

VPN > IPsec > Server Certificates (files needed for "IPsec server" mode)

CA certificate:	file 'ca-cert.pem'	Seleccionar archivo	Ningún archivo seleccionado	Upload	not uploaded
CA key:	file 'ca-key.pem'	Seleccionar archivo	Ningún archivo seleccionado	Upload	not uploaded
Server Certificate:	file 'server-cert.pem'	Seleccionar archivo	Ningún archivo seleccionado	Upload	not uploaded
Server KEY:	file 'server-key.pem'	Seleccionar archivo	Ningún archivo seleccionado	Upload	not uploaded
Client 1 Certificate:	file 'client1-cert.pem'	Seleccionar archivo	Ningún archivo seleccionado	Upload	not uploaded
Client 2 Certificate:	file 'client2-cert.pem'	Seleccionar archivo	Ningún archivo seleccionado	Upload	not uploaded
Client 3 Certificate:	file 'client3-cert.pem'	Seleccionar archivo	Ningún archivo seleccionado	Upload	not uploaded

DELETE ALL SERVER CERTIFICATES

GENERATE ALL SERVER CERTIFICATES AUTOMATICALLY

2) If no certificates are available, the TITAN-based device has a button to generate them. When you press the button, all certificates will be generated automatically. The process may take up to 5 minutes to complete. Click on the “REFRESH” button to check the status of the process.

Snmp

Tacacs+

Mqtt

Https

Audio

User Permissions

Passwords Web UI

Backup / Factory

Firmware Upgrade

Reboot

Logout

file 'server-cert.pem'

Server KEY:

file 'server-key.pem'

Client 1 Certificate:

file 'client1-cert.pem'

Client 2 Certificate:

file 'client2-cert.pem'

Client 3 Certificate:

file 'client3-cert.pem'

Seleccionar archivo	Ningún archivo seleccionado	Upload	not uploaded
Seleccionar archivo	Ningún archivo seleccionado	Upload	not uploaded
Seleccionar archivo	Ningún archivo seleccionado	Upload	not uploaded
Seleccionar archivo	Ningún archivo seleccionado	Upload	not uploaded

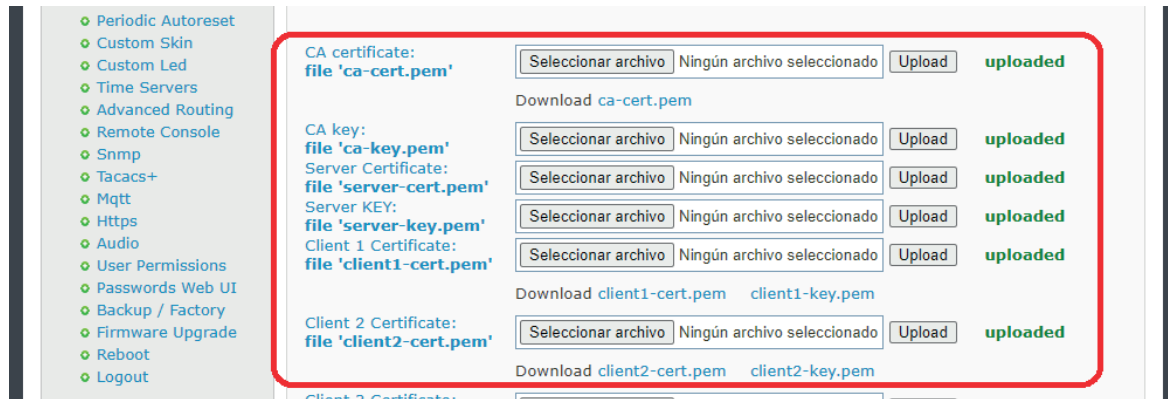
DELETE ALL SERVER CERTIFICATES

GENERATE ALL SERVER CERTIFICATES AUTOMATICALLY

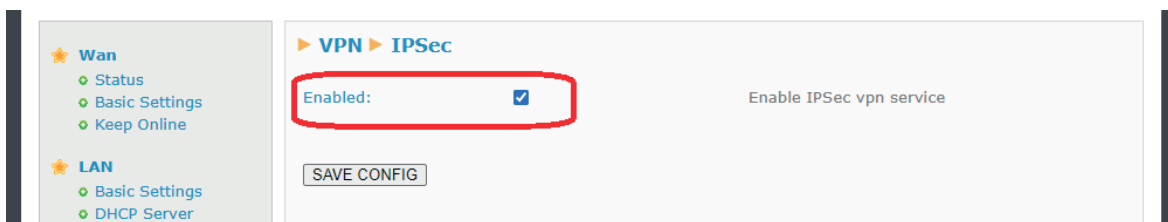
In this example, we will use the second option to generate all certificates automatically. To do this, click on the "GENERATE ALL SERVER CERTIFICATES AUTOMATICALLY" button.

NB: Make sure the router has been updated before generating the certificates.

Once the process has finished correctly, the result will be:



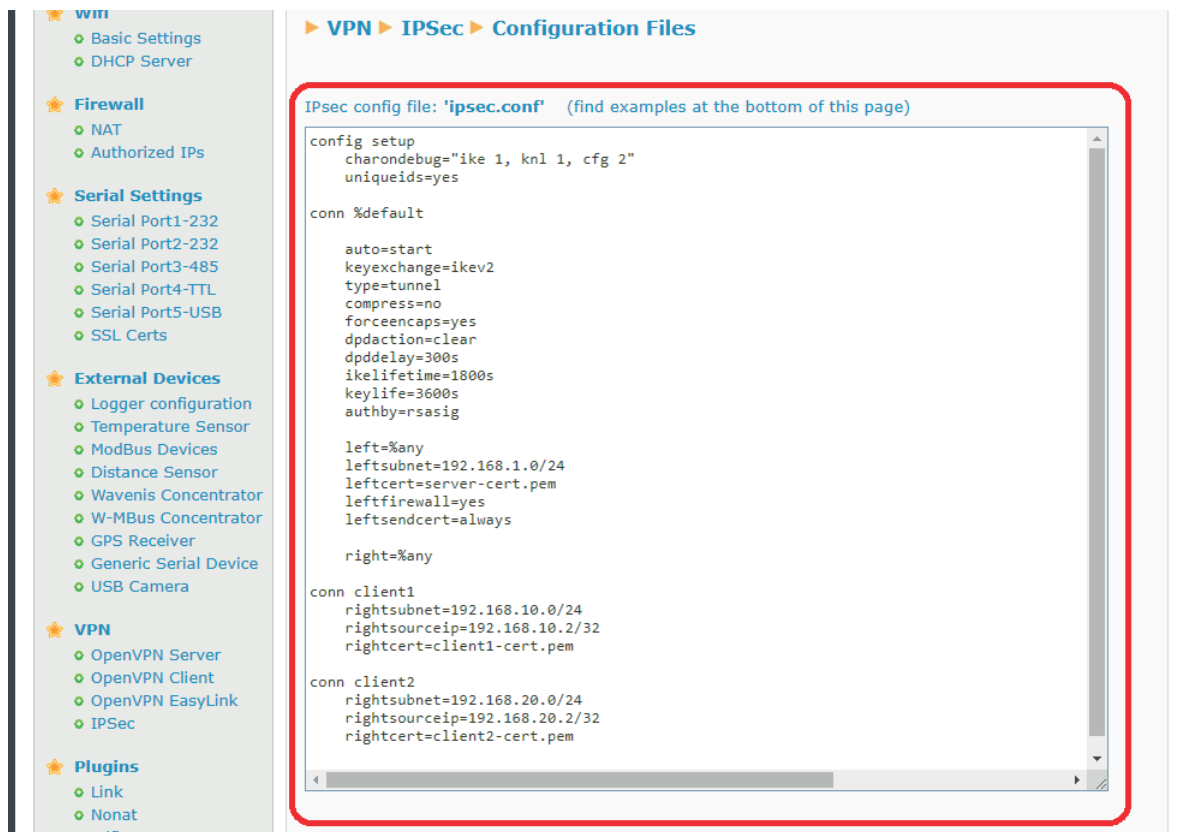
Once you have the necessary certificates, we can proceed with the actual configuration of the VPN. To do this, check the "Enabled" box at the top of the configuration page and click on the "SAVE CONFIG" button.



Lastly, since the TITAN-based device's IPSec service is based on strongswan, the "ipsec.conf" and "ipsec.secrets" files must also be configured. The simplest solution is to go to the examples at the bottom of the page and choose the example that is closest to your configuration needs. For this application note we will choose example 3 (as we are configuring the server), clicking on (downloading) the corresponding "ipsec.conf" and "ipsec.secrets" files, which we will open with a notepad to extract their contents.



This content must be tailored to the example and inserted into the appropriate box. For “ipsec.conf”:



VPN ► IPsec ► Configuration Files

IPsec config file: 'ipsec.conf' (find examples at the bottom of this page)

```
config setup
    charondebug="ike 1, knl 1, cfg 2"
    uniqueids=yes

conn %default

    auto=start
    keyexchange=ikev2
    type=tunnel
    compress=no
    forceencaps=yes
    dpdaction=clear
    dpddelay=300s
    ikelifetime=1800s
    keylife=3600s
    authby=rsasig

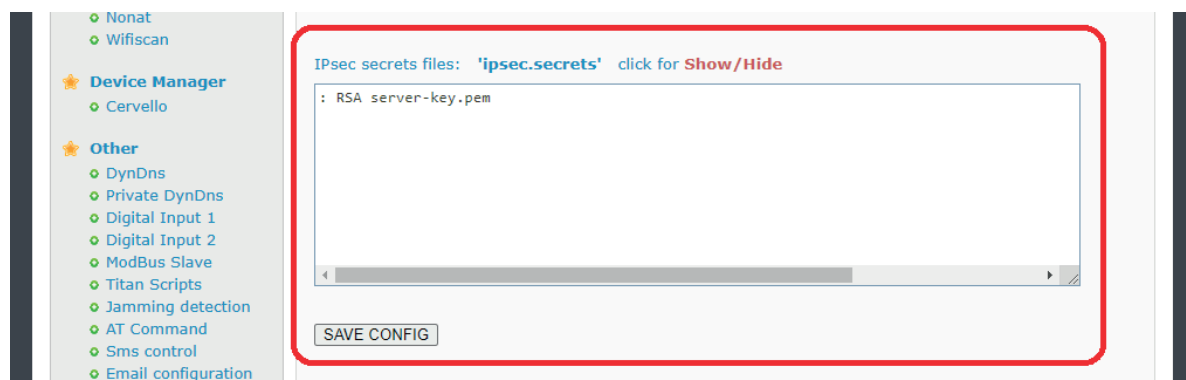
    left=%any
    leftsubnet=192.168.1.0/24
    leftcert=server-cert.pem
    leftfirewall=yes
    leftsendcert=always

    right=%any

conn client1
    rightsubnet=192.168.10.0/24
    rightsourceip=192.168.10.2/32
    rightcert=client1-cert.pem

conn client2
    rightsubnet=192.168.20.0/24
    rightsourceip=192.168.20.2/32
    rightcert=client2-cert.pem
```

And for “ipsec.secrets” (you must click on the “Show/Hide” legend beforehand to display the box):



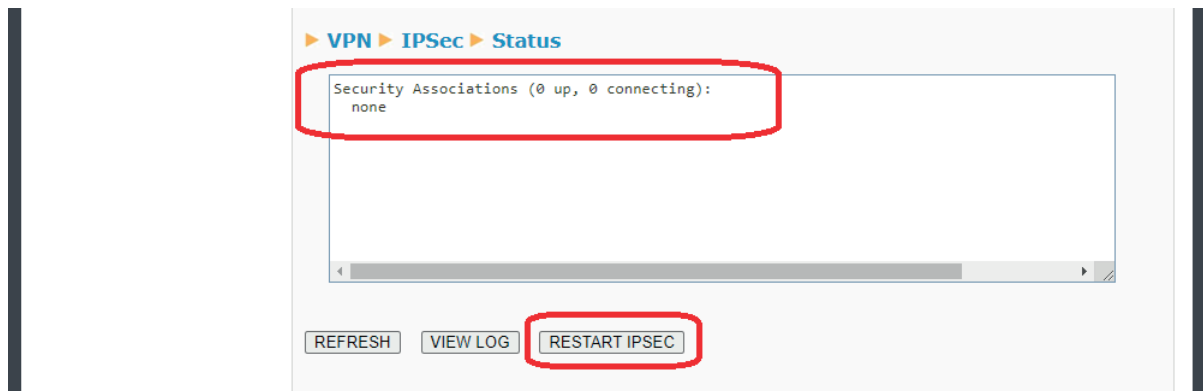
IPsec secrets files: 'ipsec.secrets' click for **Show/Hide**

```
: RSA server-key.pem
```

SAVE CONFIG

Next we click on the “SAVE CONFIG” button, which will record the contents of both files in the TITAN-based device’s internal memory. Lastly, if the IPsec service was not started when the device started (i.e. the “Enabled” box was not checked), it must be fully restarted (“Other >> Reboot” menu). If the IPsec service was already started (“Enabled” box checked), you can just click on the “RESTART IPSEC” button to restart the IPsec service with the new configuration, without having to restart the device itself, which is a much faster option.

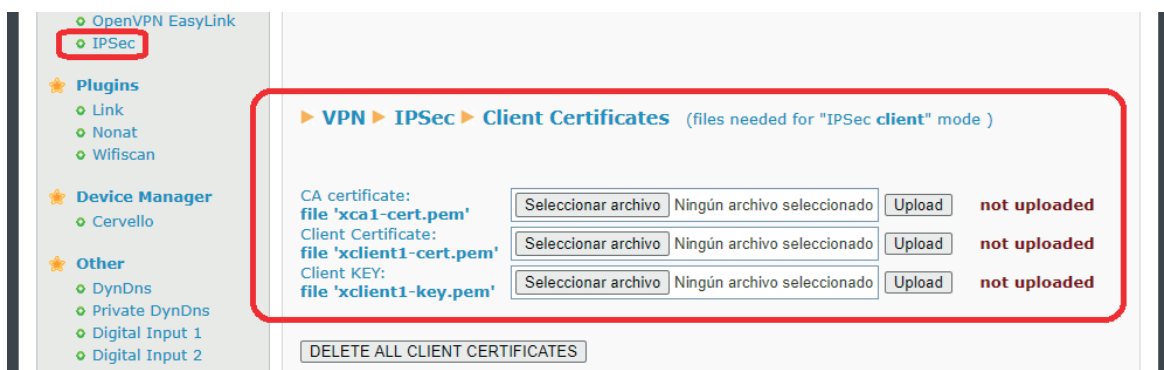
Once the device has been restarted, or the “RESTART IPSEC” button has been pressed (if the service was already active), the IPSEC connection status will appear as shown below. If the “Status” box is blank, the service may not yet have started. Wait a few seconds and click on the “REFRESH” button.



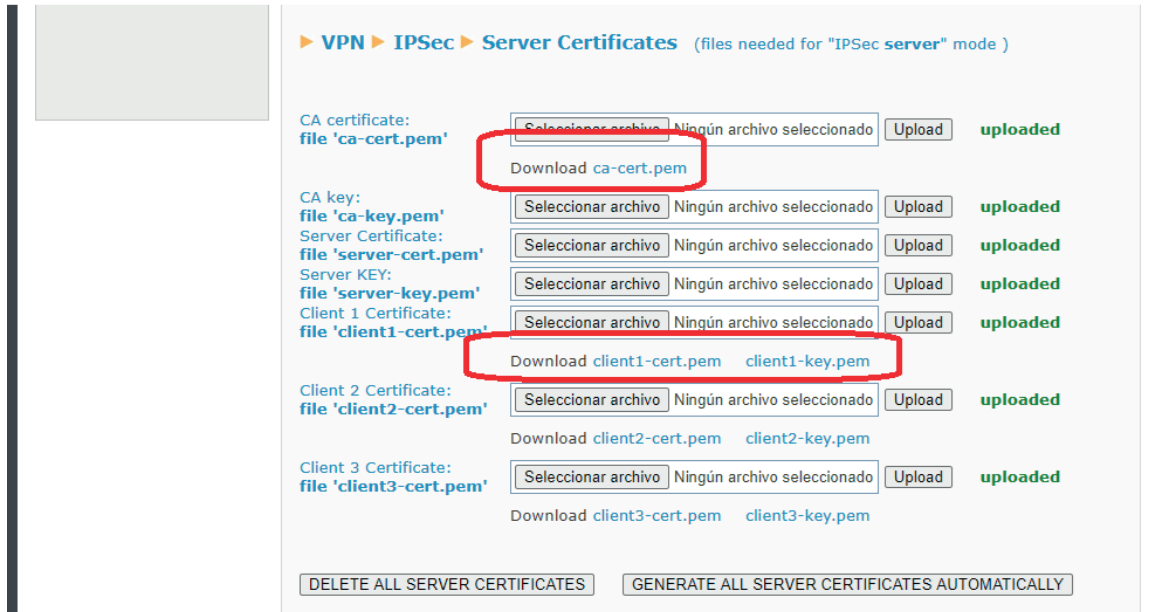
4. IPSEC configuration of the TITAN-based device (CLIENT)

In this section we can configure the TITAN-based device acting as the IPsec client and connected to PLC1. Configuring the second TITAN-based device connected to PLC2 follows the same process.

First we must go to the “VPN > IPSEC” menu. We will need the certificates related to the “Client Certificates” section.

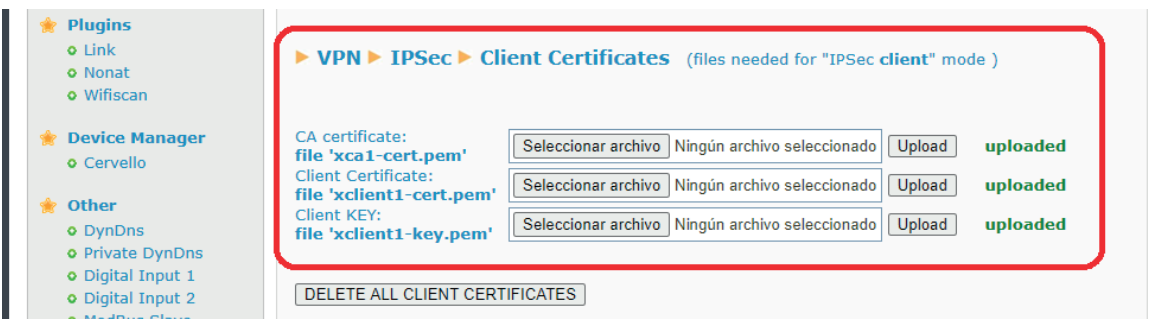


These certificates can be downloaded from the “certificates” section of the TITAN-based device acting as the IPSec Master and that were generated previously. We must download the files “ca-cert”, “client1-cert.pem” and “client1-key.pem” for the TITAN-based device connected to PLC1.

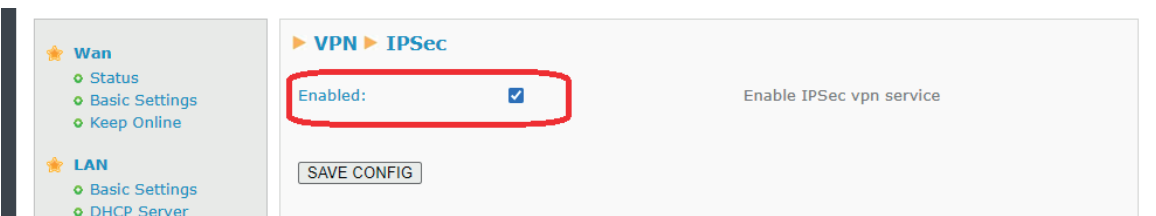


The TITAN-based device connected to PLC2 will also need the “ca-cert” files, but the ones for client2: “client2-cert.pem”, “client2-key.pem”.

Once the certificates have been uploaded to the TITAN-based device, the configuration screen will appear as follows.



Once you have the necessary certificates, we can proceed with the actual configuration of the VPN. To do this, check the “Enabled” box at the top of the configuration page and click on the “SAVE CONFIG” button.



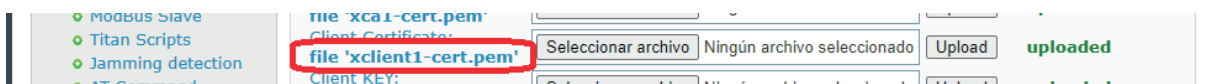
Lastly, since the TITAN-based device's IPSec service is based on strongswan, the "ipsec.conf" and "ipsec.secrets" files must also be configured. The simplest solution is to go to the examples at the bottom of the page and choose the example that is closest to your configuration needs. We will choose example 4 for this application note (as we are configuring the Client), clicking on (downloading) the corresponding "ipsec.conf" and "ipsec.secrets" files, which we will open with Notepad to extract their contents.



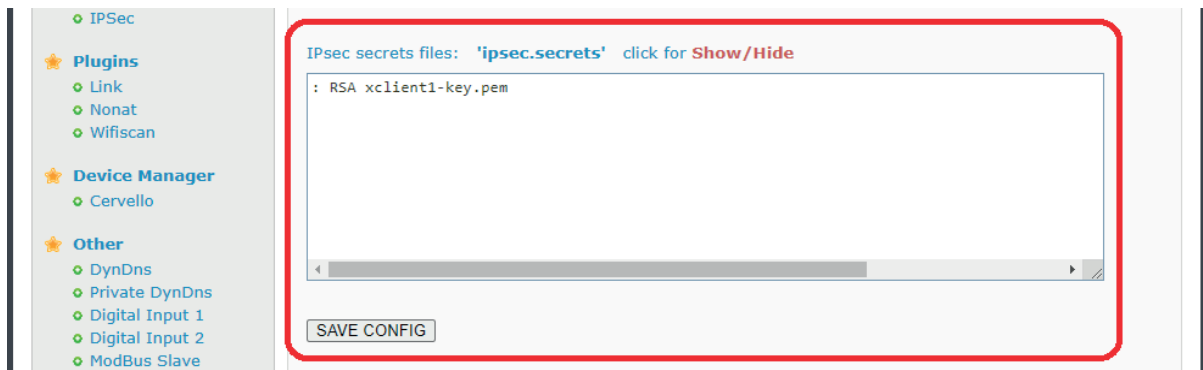
The content must be tailored to the scenario and inserted into the appropriate box. For "ipsec.conf":



Remember that in "right" you must indicate the public IP of the TITAN-based device acting as the IPSec Master, in this example it is 88.28.54.84. We must also note that the value in leftcert must be "xclient1-cert.pem" in the 2 titans acting as IPSec clients, since this is the name with which the TITAN-based device internally stores the certificate, as can be seen above and as shown in the following image.

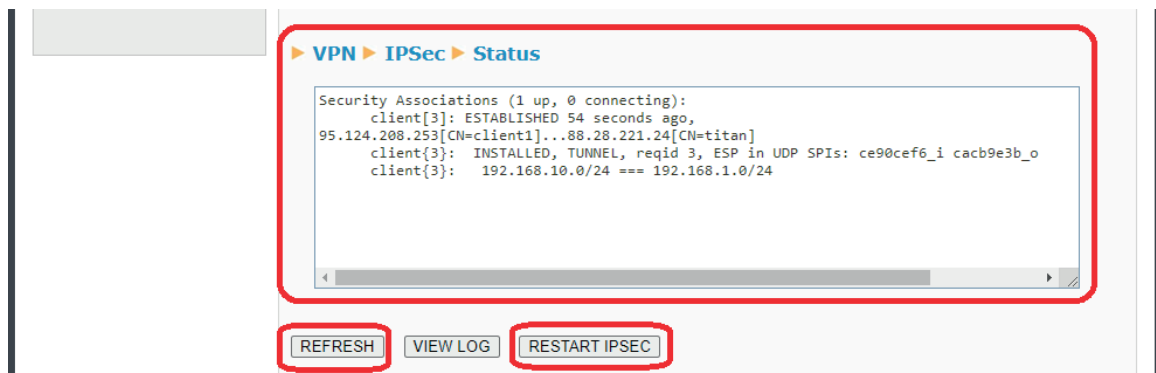


And for “ipsec.secrets” (you must click on the “Show/Hide” legend beforehand to display the box):



Next we click on the “SAVE CONFIG” button, which will record the contents of both files in the TITAN-based device’s internal memory. Lastly, if the IPsec service was not started when the device started (i.e. the “Enabled” box was not checked), it must be fully restarted (“Other> Reboot” menu). If the IPsec service was already started (“Enabled” box checked), you can just click on the “RESTART IPSEC” button to restart the IPsec service with the new configuration, without having to restart the device itself, which is a much faster option.

Once the TITAN-based equipment has been restarted or the “RESTART IPSEC” button has been pressed (if the service was already active), the IPSEC connection status will appear as shown below. If the “Status” box is blank, the service may not yet have started. Wait a few seconds and click on the “REFRESH” button. If everything works fine, you should see a screen like the one below:



At this point, PLC1 (client) and PLC3 (server) can already interact with each other through a secure IPsec tunnel. Repeat the same procedure for the TITAN-based device connected to PLC2.